



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,959	11/30/2001	Mark Muhlestein	5693P272X	5673
48102 7590 01/10/2008 NETWORK APPLIANCE/BLAKELY 1279 OAKMEAD PARKWAY SUNNYVALE, CA 94085-4040			EXAMINER KHOSHNOODI, NADIA	
			ART UNIT 2137	PAPER NUMBER
			MAIL DATE 01/10/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/010,959

Applicant(s)

MUHLESTEIN, MARK

Examiner

Nadia Khoshnoodi

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 76-89 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 76-89 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 March 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 3/10-18-2007.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claims 1-75 have been cancelled. Applicant's arguments/amendments with respect to newly presented claims 76-89 filed 10/18/2007 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Drawings

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the step of determining whether to cause the processing device to perform the operation based at least partially on a file space containing the object, must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an

application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 82 is objected to because of the following informalities:

In line 10 of the claim ("least partially on and a file space containing the object") the 'and' should be deleted.

In lines 13-14 of the claim ("determination, to cause the processing device access the object stored at the storage server and perform the operation"), the limitation should be changed so that it is similar to the following statement "determination, to cause the processing device to access the object stored at the storage server and to perform the operation."

Appropriate correction is required.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

II. Claims 76, 79-80, and 82-84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithson et al., US Patent No. 6,802,012, and further in view of Edwards et al., US Patent No. 6,931,540.

As per claim 76:

Smithson et al. substantially teach a method including: receiving at a storage server, from a requester, a request for an object stored at the server (col. 4, lines 25-30); in response to the request, determining whether to cause a processing device access to the object, wherein the processing device is separate from the storage server and is not in a path from the requester to the object (col. 4, lines 31-39); causing the processing device to perform the operation in response to a specified outcome of said determining (col. 4, lines 40-43); receiving at the storage server a result of the operation from the processing device (col. 4, lines 40-43); and conditionally allowing access to the object in response to the request according to the result of the operation (col. 4, lines 43-45).

Not explicitly disclosed is wherein the determining step includes determining at the storage server whether to cause a processing device to access the object stored at the storage server and perform an operation on data associated with the object based at least partially on a file space containing the object. However, Edwards et al. teach that various processing devices perform various scan types depending on the type of file which is requested to be scanned (col. 5, lines 1-12 and lines 35-39). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. to determine whether a processing device has proper access to perform a particular virus scan on the file at hand. This modification would have been obvious because a person having ordinary skill in the

art, at the time the invention was made, would have been motivated to do so since Edwards et al. suggest that varying levels of security are utilized depending on the process accessing the file, as well as the type of file being accessed in order to allow for better/more efficient use of the systems resources in col. 3, line 60 – col. 4, line 10.

As per claim 79:

Smithson et al. and Edwards et al. substantially teach the method of claim 76.

Furthermore, Edwards et al. teach wherein the storage server enforces a timeout for the operation; wherein even if the timeout expires, the processing device completes the operation and reports the result of the operation to the server; and wherein the storage server stores the result of the operation for possible later use (col. 5, lines 1-5 and col. 6, lines 49-57).

As per claim 80:

Smithson et al. and Edwards et al. substantially teach the method of claim 76.

Furthermore, Smithson et al. teach wherein the operation comprises virus scanning (col. 4, lines 30-32).

As per claim 82:

Smithson et al. substantially teach an apparatus comprising: a storage server storing a set of objects and having a network interface (col. 4, lines 25-33); and a processing device that is connected to the storage server and that is not in a path from a client to the objects stored at the server (col. 4, lines 31-39), wherein when the storage server receives a client request for an object of the set of objects through the network interface (col. 4, lines 25-33); the storage server sends a first message to the processing device that indicates the object to the processing device, in response to a specified outcome of the determination, to cause the processing device access

the object stored at the storage server and perform the operation (col. 4, lines 32-39); the processing device sends a second message to the storage server that indicates a result of the operation (col. 4, lines 40-43); and the storage server generates a response to the client request, the response conditionally providing access by the client to the object according to the second message (col. 4, lines 43-45).

Not explicitly disclosed is wherein the storage server determines whether to cause the processing device to perform an operation on data associated with the object, wherein the storage server determines whether to cause the processing device to perform the operation based at least partially on and a file space containing the object. However, Edwards et al. teach that various processing devices perform various scan types depending on the type of file which is requested to be scanned (col. 5, lines 1-12 and lines 35-39). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. to determine whether a processing device has proper access to perform a particular virus scan on the file at hand. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Edwards et al. suggest that varying levels of security are utilized depending on the process accessing the file, as well as the type of file being accessed in order to allow for better/more efficient use of the systems resources in col. 3, line 60 – col. 4, line 10.

As per claim 83:

Smithson et al. and Edwards et al. substantially teach the apparatus of claim 82. Furthermore, Edwards et al. teach wherein the storage server enforces a timeout for the second message; wherein even if the timeout expires, the second message is sent from the processing

device to the server; and wherein the storage server stores the result of the operation for possible later use (col. 5, lines 1-5 and col. 6, lines 49-57).

As per claim 84:

Smithson et al. and Edwards et al. substantially teach the apparatus of claim 82.

Furthermore, Smithson et al. teach wherein the operation comprises virus scanning (col. 4, lines 30-32).

III. Claim 77 is rejected under 35 U.S.C. 103(a) as being unpatentable over Smithson et al., US Patent No. 6,802,012, and Edwards et al., US Patent No. 6,931,540, as applied to claim 76 above, and further in view of Tso et al., US Patent No. 6,088,803.

As per claim 77:

Smithson et al. and Edwards et al. substantially teach the method of claim 76.

Furthermore, Edwards et al. teach wherein the operation includes a plurality of processes (col. 3, lines 60-66). Not explicitly disclosed is each process being performed at a separate processing device in a cluster. However, Tso et al. teach that there may be several content servers carrying the data objects and that each one of the processing devices capable of performing virus scanning may be distributed across a network (col. 2, lines 38-45). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. and Edwards et al. to have a separate processing device for the various types of virus scans that may be performed on a file, where those processing devices would form a cluster. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Tso et al.

suggest that distributed virus scanning ensures the security of networked elements in col. 8, lines 50-62.

IV. Claims 78, 81, and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithson et al., US Patent No. 6,802,012, and Edwards et al., US Patent No. 6,931,540, as applied to claim 76 above, and further in view of ***.

As per claim 78:

Smithson et al. and Edwards et al. substantially teach the method of claim 76.

Furthermore, Edwards et al. teach the method further including assigning a specific access type to the processing device by the server, the specific access type allowing the processing device to perform the operation (col. 3, lines 45-59). Not explicitly disclosed is wherein the specific access type allows the processing device to perform the operation even while another user has a lock on the object. However, Pouban et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pouban et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

As per claim 81:

Smithson et al. and Edwards et al. substantially teach the method of claim 80.

Furthermore, Smithson et al. teach wherein the operation is performed only if the processing device has open-for-scanning permission to access the object (col. 4, lines 50-63). Not explicitly disclosed is wherein if the processing device has the open-for-scanning permission to access the object, the operation is performed even if the object is locked by another user. However, Pouban et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pouban et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

As per claim 85:

Smithson et al. and Edwards et al. substantially teach the apparatus of claim 84.

Furthermore, Smithson et al. teach wherein the operation is performed only if the processing device has open-for-scanning permission to access the object (col. 4, lines 50-63). Not explicitly disclosed is wherein if the processing device has the open-for-scanning permission to access the

object, the operation is performed even if the object is locked by another user. However, Pouban et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pouban et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

V. Claims 86-89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithson et al., US Patent No. 6,802,012 and further in view of Pouban et al., US Patent No. 4,104,718.

As per claim 86:

Smithson et al. substantially teach a method including: receiving at a storage server a client request for an object stored at the server (col. 4, lines 25-30); assigning by the storage server a specific access type to a processing device that is separate from the storage server and is not in a path from the client to the object (col. 4, lines 30-39 and lines 56-67); causing the processing device to perform the operation (col. 4, lines 40-43); receiving at the storage server a result of the operation from the processing device (col. 4, lines 40-43); and conditionally

allowing access to the object in response to the client request according to the result of the operation (col. 4, lines 43-45).

Not explicitly disclosed is that the specific access type allows the processing device to perform an operation on the object even while another client has a lock on the object. However, Pouban et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pouban et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

As per claim 87:

Smithson et al. and Pouban et al. substantially teach the method of claim 86. Furthermore, Smithson et al. teach wherein the operation comprises virus scanning (col. 4, lines 30-32).

As per claim 88:

Smithson et al. substantially teach an apparatus comprising: a storage server storing a set of objects and having a network interface (col. 4, lines 25-33); and a processing device coupled

to the server, wherein the processing device is not in a path from a client to the objects stored at the server, wherein: the storage server receives a client request for an object of the set of objects through the network interface (col. 4, lines 30-39); the storage server assigns a specific access type to a processing device that is separate from the storage server and is not in a path from the client to the object (col. 4, lines 56-67); the storage server causes the processing device to perform the operation (col. 4, lines 40-43); the storage server receives at the storage server a result of the operation from the processing device (col. 4, lines 40-43); and the storage server conditionally allows access to the object in response to the client request according to the result of the operation (col. 4, lines 43-45).

Not explicitly disclosed is that the specific access type allows the processing device to perform an operation on the object even while another client has a lock on the object. However, Pouban et al. teach that it is well known that, depending on the particular lock the user has put on the file, reading of the file is still permitted by other processes (where virus-scanning is a "read"-type operation as opposed to a "write" operation). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Smithson et al. and Edwards et al. to allow for the processing device to perform an operation, such as virus scanning on the object even while another user has a lock on the object. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pouban et al. suggest that if a "for input" lock is the type of lock placed on a file by a user, other processes may still access the file for reading purposes, where this is beneficial so that authorized users may access resources as needed for their duties in col. 63, lines 57-63.

As per claim 89:

Smithson et al. and Poublan et al. substantially teach the apparatus of claim 88.

Furthermore, Smithson et al. teach wherein the operation comprises virus scanning (col. 4, lines 30-32).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

Application/Control Number:
10/010,959
Art Unit: 2137

Page 14

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Nadia Khoshnoodi
Nadia Khoshnoodi
Examiner
Art Unit 2137
1/5/2008

NK

Cynthia Britt
CYNTHIA BRITT
PRIMARY EXAMINER
1-6-08